I. Amendments to the Claims

Please amend the claims as follows with the following version of the claims in accordance with revised 37 CFR § 1.121.

1. (Currently Amended) A method for acquiring public-key infrastructure (PKI) credentials for a user, the method comprising:

~~generating a pre-registration record for the user;~~

receiving a ~~sending the~~ pre-registration record as an e-mail attachment in an e-mail message to the user at a client;

in response to receiving the pre-registration record, prompting the user at the client for user authentication data;

generating at the client a cryptographic key pair comprising a user private key and a user public key;

sending a PKI credential request for the PKI credentials to a certificate issuing authority, wherein the public key certificate request comprises the pre-registration record, ~~and~~ the user public key, and the user authentication data; and

receiving the PKI credentials at the client, wherein the PKI credentials comprise a public key certificate for the user and an attribute certificate for the user, wherein the attribute certificate comprises the user authentication data.

2. (Original) The method of claim 1 further comprising:

retrieving user information from a directory; and

storing the user information into the pre-registration record.

3. (Original) The method of claim 1 further comprising:

viewing the e-mail message within a browser, wherein the browser generates the cryptographic key pair; and

storing the user private key in a secure local keystore at the client by the browser.

4. (Original) The method of claim 1 wherein the e-mail message is formatted according to an Secure/Multipurpose Internet Mail

Extensions (S/MIME) standard.

5. (Canceled).

6. (Original) The method of claim 1 further comprising:

retrieving a Uniform Resource Identifier (URI) from the e-mail message; and

posting the public key certificate request to the certificate issuing authority using the URI.

7. (Original) The method of claim 1 further comprising:

storing the PKI credentials in a secure local keystore at the client.

8. (Canceled).

9. (Original) The method of claim 1 further comprising:

publishing the PKI credentials in a directory.

10. (Original) The method of claim 1 wherein the PKI credentials are formatted according to an X.509 standard.

11. (Currently Amended) An apparatus for acquiring public-key infrastructure (PKI) credentials for a user, the apparatus comprising:

~~means for generating a pre-registration record for the user;~~

means for receiving a ~~sending the~~ pre-registration record as an e-mail attachment in an e-mail message to the user at a client;

means for prompting the user at the client for user authentication data in response to receiving the pre-registration record;

means for generating at the client a cryptographic key pair comprising a user private key and a user public key;

means for sending a PKI credential request for the PKI credentials to a certificate issuing authority, wherein the public key certificate request comprises the pre-registration record, ~~and~~ the user public key, and the user authentication data; and

means for receiving the PKI credentials at the client, wherein the PKI credentials comprise a public key certificate for the user and an attribute certificate for the user, wherein the attribute certificate comprises the user authentication data.

12. (Original) The apparatus of claim 11 further comprising:

means for retrieving user information from a directory; and

means for storing the user information into the pre-registration record.

13. (Original) The apparatus of claim 11 further comprising:

means for viewing the e-mail message within a browser, wherein the browser generates the cryptographic key pair; and

means for storing the user private key in a secure local keystore at the client by the browser.

14. (Original) The apparatus of claim 11 wherein the e-mail message is formatted according to an Secure/Multipurpose Internet Mail Extensions (S/MIME) standard.

15. (Canceled).

16. (Original) The apparatus of claim 11 further comprising:

means for retrieving a Uniform Resource Identifier (URI) from the e-mail message; and

means for posting the public key certificate request to the certificate issuing authority using the URI.

17. (Original) The apparatus of claim 11 further comprising:

means for storing the PKI credentials in a secure local keystore at the client.

18. (Canceled).

19. (Original) The apparatus of claim 11 further comprising:

means for publishing the PKI credentials in a directory.

20. (Original) The apparatus of claim 11 wherein the PKI credentials are formatted according to an X.509 standard.

21. (Currently Amended) A computer program product in a computer-readable medium for use in a data processing system for acquiring public-key infrastructure (PKI) credentials for a user, the computer program product comprising:

~~instructions for generating a pre-registration record for the user;~~

instructions for receiving a ~~sending the~~ pre-registration record as an e-mail attachment in an e-mail message to the user at a client;

instructions for prompting the user at the client for user authentication data in response to receiving the pre-registration record;

instructions for generating at the client a cryptographic key pair comprising a user private key and a user public key;

instructions for sending a PKI credential request for the PKI credentials to a certificate issuing authority, wherein the public key certificate request comprises the pre-registration record, and the user public key, and the user authentication data; and

instructions for receiving the PKI credentials at the client, wherein the PKI credentials comprise a public key certificate for the user and an attribute certificate for the user, wherein the attribute certificate comprises the user authentication data.

22. (Original) The computer program product of claim 21 further comprising:

instructions for retrieving user information from a directory; and

instructions for storing the user information into the pre-registration record.

23. (Original) The computer program product of claim 21 further comprising:

instructions for viewing the e-mail message within a browser, wherein the browser generates the cryptographic key pair; and

instructions for storing the user private key in a secure local keystore at the client by the browser.

24. (Original) The computer program product of claim 21 wherein the e-mail message is formatted according to an Secure/Multipurpose Internet Mail Extensions (S/MIME) standard.

25. (Canceled).

26. (Original) The computer program product of claim 21 further comprising:

instructions for retrieving a Uniform Resource Identifier (URI) from the e-mail message; and

instructions for posting the public key certificate request to the certificate issuing authority using the URI.

27. (Original) The computer program product of claim 21 further comprising:

instructions for storing the PKI credentials in a secure local keystore at the client.

28. (Canceled).

29. (Original) The computer program product of claim 21 further comprising:

instructions for publishing the PKI credentials in a directory.

30. (Original) The computer program product of claim 21 wherein the PKI credentials are formatted according to an X.509 standard.

II. General Remarks Concerning This Response

Claims 1-4, 6, 7, 9-14, 16, 17, 19-24, 26, 27, 29, and 30 are currently pending in the present application. Claims 1, 11, and 21 have been amended; no claims have been added; and claims 5, 8, 15, 18, 25, and 28 have been canceled in this response. Reconsideration of the claims is respectfully requested.

III. Summary of Present Invention

A methodology is presented for securely acquiring and managing PKI credentials using an enterprise's pre-existing information technology. A management application places user information from a directory into a pre-registration record, which is sent to the user as an e-mail attachment. When the user views the e-mail message through a browser-type application that has built-in key generation and digital certificate management, the user may be prompted for additional information, such as passwords. The browser-type application then generates a public/private key pair and stores the private key in a secure local keystore while also securely sending the public key, authentication data, and pre-registration record to a registration/certificate authority. A public key certificate and an attribute certificate are then issued for the user, copies of which are published into the directory and returned to the user for storing within the user's secure local keystore. The certificates may then be used in typical manners.